REMARKS

Claims 1-45 are pending in the application. Independent claim 1 is amended herein to recite features of dependent claims 9 and 10. Claim 9 is cancelled and claim 10 is amended to remove subject matter added to claim 1. Claims 4 and 6 are amended for consistency with independent claim 1.

Similarly, independent claim 16 is amended herein to recite features of dependent claims 24 and 25. Claim 24 is cancelled and claim 25 is amended to delete repetitive features. Claims 19 and 21 are amended for consistency with independent claim 16.

Similarly, independent claim 31 is amended herein to recite features of dependent claims 39 and 40. Claim 39 is cancelled and claim 40 is amended to delete repetitive features. Claims 34 and 36 are amended for consistency with independent claim 31.

The independent claims are also amended with regard to formatting by moving the recited "wherein the ephemeral key pair" clause into paragraph a). Claims 4, 19, and 34 are amended for clarity to better tie the recited generator *G* to the respective claims. It is respectfully submitted that the subject matter of this amendment was implied by the prior claim language and that this amendment is not substantive. Claims 10 and 40 are amended for clarity to edit potentially confusing notation. It is respectfully submitted that these amendments are not substantive.

These amendments should be entered and given full consideration for two reasons. First, the amendments incorporate subject matter from dependent claims that have previously been addressed by the office. Thus, no further search should be required. Second, in a telephone interview on June 3, 2009, assignee requested clarification as to where Schneier contained a teaching of ephemeral keys. The examiner stated that she could not remember why she

considered Schneier to teach ephemeral keys. Assignee was advised to file remarks arguing that Schneier does not teach ephemeral keys and the rejection would subsequently be withdrawn. Assignee filed such remarks on June 19, 2009. It appears that the examiner subsequently recalled her position and maintained the rejection. The current amendments should be entered and considered because the assignee did not previously amend the claims in reliance on the examiner's confirmation, later retracted, that Schneier does not disclose ephemeral keys.

Claim Rejections – 35 U.S.C. § 103(a)

On page 3 of the office action, independent claims 1, 16, and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier (U.S. Patent No. 5,956,404) in view of the Perez memo. Reconsideration is respectfully requested in light of the amendments contained herein and the following remarks.

Claim 1 has been amended to recite features of dependent claims 9 and 10. Specifically, claim 1 now recites:

> wherein the digital signature comprises a first value *r* and a second value *s*, the process further comprising the step of, at the sender, transmitting an encryption ephemeral public key *X*, the ciphertext message, and the second value *s* of the digital signature to the receiver;
>
> wherein the first value *r* of the digital signature is calculated at the receiver using a decrypted form of the plaintext message and the transmitted encryption ephemeral public key *X* and validating the digital signature based on the calculated first value *r* and the transmitted second value *s*

In rejecting claims 9 and 10, the office action cites to the general public-private key encryption description at col. 1 lines 45-65 of Schneier as teaching the claimed features. It is respectfully submitted that the very general description of col. 1 of Schneier does not teach or suggest the detailed features contained in amended claim 1, especially the lack of a transmission of *r* from the sender to the receiver and the calculation of *r* at the receiver.

The differences between the prior mechanisms, described in col. 1 of Schneier and depicted in FIG. 3 of the application at issue, and the process of claim 1, an example of which is shown in FIG. 4, is described in detail at page 9, line 22 to page 10, line 18 of the current application, which states:

> The present invention outlined in Fig. 4 deviates from the prior art scheme of Fig. 3 in several important aspects. The improved digital signature scheme of the present invention uses the encryption ephemeral key pair (X, x) produced in the encryption stage 50' as a substitute for the signature ephemeral key pair (Z, z) required in the digital signature stage 70'. The value of signature ephemeral private key z 34' is set to the value of encryption ephemeral private key x from the encryption stage. Consequently, the random generation of z and the computation of Z 36' are not required since signature ephemeral public key Z 36' equals encryption ephemeral public key X 20. Advantageously, this reduces the computational load on the sender. In essence, the value for x is used for two different purposes. In the first instance, x is used for the encryption process scheme 50'. In the second instance, the x is also used in the digital signature scheme 70'.
>
> After transmission of the encryption public key X 20, ciphertext 22 and signature s 38', Bob may then calculate secret key $K = bX$ and then decrypt the message by *message =decrypt (K, ciphertext)*. The digital signature scheme then preferably hashes the message 40 to calculate h, as indicated in block 42'. Two pieces of information for the digital signature still need to be computed, namely integers r and s. The integers are calculated as follows: $r = Z^* + h \bmod n = X^* + h \bmod n$ and $s = z - ar \bmod n = x - ar \bmod n$. **However, only s in addition to the encryption ephemeral public key X and the ciphertext must be transmitted to Bob in the inventive scheme 80'. Rather than r being transmitted to Bob, r is instead reconstructed at the receive side by calculating $r = X^* + h \bmod n$. In this manner, the overall byte-size overhead associated with the digital signature 38' is reduced by not transmitting r. In a specific embodiment of the invention, the saving was in the range of twenty-two bytes. In portable two-way wireless communication devices, reducing the transmission by twenty-two bytes is considerably useful and advantageous.** (emphasis added)

Because the general public-private key disclosure of col. 1, lines 45-65 of Schneier does not teach or suggest the detailed features incorporated into claim 1, and the office action makes no allegation of such a teaching being found in Perez, it is respectfully requested that the § 103 rejection of claim 1 be withdrawn.

Similar amendments have been made to independent claims 16 and 31, which are rejected for similar reasons as offered for claim 1. It is respectfully requested that the § 103 rejections of these claims be withdrawn for similar reasons as offered for claim 1.

It is noted that the assignee has not, at this time, presented arguments with respect to certain dependent claims in the instant application. The assignee nevertheless reserves the right to argue the patentability of these dependent claims in the instant application at a future time, should that become necessary.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issue.

Respectfully submitted,

Date: 19 November 2009

By: 

Matthew W. Johnson
Reg. No. 59,108
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(412) 394-9524